**REMARKS**

This paper responds to the first Office action, which was non-final.

The undersigned notes that all previous art-related rejections have been overcome as a result of the paper submitted May 19, 2008. The Examiner is thanked for withdrawing those rejections.

Claims 19-21 and 23-27 once again are rejected under 35 U.S.C. § 101 as directed to non-statutory subject matter. The Examiner's rejection is not directed to the format of the claims themselves; rather, the inclusion of "transmission-type media" in the written description (in the paragraph bridging pages 26-27) as a type of "computer readable medium" is deemed to render the claim non-statutory. While it is true that the scope of the claims is informed by the written description, this rejection appears to be misplaced, as it does not afford due consideration to the actual wording of the claims. In particular, the Examiner will note that the preamble of claim 19 refers not just to a "computer readable medium," but rather a "computer program product in a computer readable medium for use at a proxy server." Nevertheless, to reduce the number of contested issues here, the written description has been amended at pages 26-27 to remove the explicit reference associating transmission functionality with the "computer readable medium." Accordingly, the Examiner is requested to withdraw the § 101 rejection.

For the same reason, the Examiner is requested the new rejection under 35 U.S.C. § 112, for alleged lack of enablement.

The pending claim are newly rejected under 35 U.S.C. §103(a) as being unpatentable over Nilsson et al (WO 99/64967) in view of Internet Request for Comment (RFC) 2965 (hereinafter "RFC").

Nilsson illustrates a proxy server 66 located between a mobile device user terminal 52 having a browser 54, and a server 70. In Nilsson, the goal is to intercept and store a cookie generated by the server 70 so that the user terminal 52 does not need to store the cookie. In operation, the client makes a request to the server, which then provides a response together with the cookie. This is a conventional server operation. Rather than passing the cookie back to the user terminal, the cookie is stored in the proxy together with information identifying the requested URL and the user terminal. In that manner, "the next time" the user terminal 52 accesses the server 70, the proxy server 66 matches the requested URL and the identification

information and in this manner finds the previously-stored cookie. The cookie is then provided to the server 70 with the request. Thus, the cookie is stored in the proxy server 66 and need not be transmitted over a wireless interface.

The RFC is cited for its alleged teaching of a "set of parameters," with reference in particular to paragraph 3.3.4. This section of the RFC describes "Sending Cookies to the Origin Server" and is a description of how a client user agent (a web browser) may include a cookie request header if it has stored cookies that are applicable to the request. According to the RFC, the cookie request header may be based on the request-host and request-port, the request URL, and the cookie's age. The syntax for the cookie request header is described and includes various attributes and values.

Respectfully, the obviousness rejection is traversed.

The subject matter of this application relates generally to a privacy proxy server or privacy service. As previously explained, if a user of such a system or service is very mobile and uses many different client devices, there may be occasions or environments in which the user would like to receive some or all cookies at a client device while filtering out some or all cookies in a different environment or on a different occasion, even though the user may or may not continue to employ a privacy proxy or privacy service in these different environments or upon these different occasions. For example, if a user only accesses a certain web site from the user's personal laptop and never from an office desktop, then the user may want to allow cookies through the privacy proxy server to the laptop; the laptop would tend to have the latest cookies stored in its cookie cache, which might be important for certain sites that are highly customized or individualized. In this example, the user's laptop would have recent cookies if the user decided to use the laptop without accessing the Web through the privacy proxy server. With the subject matter described herein, the user is able to create different client profiles based on the user's needs, thereby giving the user a finer granularity of control over the cookie filtering functionality of a privacy proxy server or a privacy service. With the described subject matter, the user can customize the operation of the privacy proxy server or the privacy service on the basis of the device that the user is using, on the basis of the user's location, or on the basis of some other type of user-configured category. For example, the user might have client profiles based on a type of client device, such as laptop vs. desktop vs. PDA, or based on client location,

such as office vs. mobile vs. home. The subject matter disclosed herein in particular allows a user to configure a privacy proxy that is located between a client device that is being operated by the user and a server that is supporting resources that are being accessed by a user. The privacy proxy filters cookies that are returned by the server in accordance with user-configurable parameters.

The "user-configurability" subject matter is incorporated into the independent claims. In particular, each independent claim positively recites the steps of receiving and storing a set of parameters, wherein the parameters comprise "domain identifiers associated with indications of whether to block transmission of cookies associated with the domain identifiers." As positively recited, the set of parameters are configured by the user at the client. In one illustrated embodiment, the user interfaces (FIGs. 4A-4C) can be used for this purpose.

With respect, the Examiner has erred in applying Nilsson to the claimed subject matter.

In particular, the Examiner argues (at page 4, lines 15-16) that Nilsson performs the step of "extracting from the response message a domain identifier associated with the server." This is incorrect; what actually happens at the Nilsson proxy server 66 is the exact opposite step, because at this point in the Nilsson processing the proxy 66 operates on the request message from the end user terminal and not the response message from the server 70. This distinction is clear from the very portion of the Nilsson text relied upon by the Examiner, namely, the text at page 3, lines 9-11 (emphasis supplied):

"Thus, when a remote HTTP server or the like is contacted by a user terminal and the remote server transmits a cookie to the user terminal, the cookie is intercepted and stored in the proxy server. Information regarding the remote server, e.g., its URL[,] and an identification identifying the user terminal or the user is stored together with the cookie. The next time the user terminal or the user accesses the same HTTP server the proxy server matches the requested URL and the identification information and in this manner finds the stored cookie. The cookie is then added to the request message so that the remote server is accessed with a copy of the cookie as desired."

At this stage in the Nilsson operation, the "domain identifier" – if any – is the URL in the request message, as opposed to the domain identifier in any server response message. Thus, the portion of the text relied upon by the Examiner does not meet the claim limitation itself.

Moreover, the final step of claim 1 requires "processing the cookie at the proxy server in accordance with the retrieved set of parameters and the extracted domain identifier." As noted in the previous paragraph, the "extracted domain identifier" referenced at this part of the claim refers to the prior "extracting" step where the "domain identifier" is extracted from the server response message; as noted above, the URL obtained by the proxy at this point in the Nilsson operation is an identifier taken from the end user request message itself. In other words, in the Nilsson operation (and after the cookie is stored at the proxy), when the end user terminal issues a next request to the server, the proxy determines whether there is a stored cookie and, if so, the proxy merely attaches the cookie to the request before passing the request to the server. The cookie itself is not processed "in accordance with [any] retrieved set of parameters and the extracted domain identifier." Stated another way, in Nilsson at most what happens is that the cookie is re-attached to the end user terminal request before that request is passed on to the server.

Further, the Examiner is reminded that the "set of parameters" referenced in the claim are parameters that "are configured by the user at the client." In concluding that this feature is present in the RFC, the Examiner has glossed over the "by the user" portion of the phrase. There is nothing in the RFC (which is an Internet standard specification) that discusses having "the user" configure a set of parameters. As noted above, and as described in the written description, this portion of the claim refers to the disclosed feature whereby the user (himself or herself) is able to create different client profiles based on the user's needs. This feature affords the user a finer granularity of control over the cookie filtering functionality of a privacy proxy server or a privacy service. As noted above, the user can customize the operation of the privacy proxy server or the privacy service on the basis of the device that the user is using, on the basis of the user's location, or on the basis of some other type of user-configured category. The user might have client profiles based on a type of client device, such as laptop vs. desktop vs. PDA, or based on client location, such as office vs. mobile vs. home. The limitation directed to "the set of parameters are configured by the user at the client" was meant to emphasize this feature.

The RFC does not disclose or suggest user-configurable parameters, and the Examiner has admitted (correctly, as it were) that Nilsson "is silent on disclosing explicitly, [a] set of parameters or wherein the set of parameters are configured by the user at the client." See, Office

action, at page 5, lines 1-2. Thus, any permissible combination of Nilsson and the RFC is not the subject matter as a whole of any independent claim as required for a prima facie case of obviousness under 35 U.S.C. § 103(a). For this reason alone, the rejection should be withdrawn, as it is the Office's burden to establish the prima facie case in the first instance.

Further, neither Nilsson nor the RFC disclose proxy server filtering of a cookie that is being returned from a server to a client, let alone per-domain cookie filtering. And more to the point, neither Nilsson nor the RFC teach enabling the proxy to receive and store "a set of [user-configured] parameters," where the parameters comprise "domain identifiers associated with indications of whether to block transmission of cookies associated with the domain identifiers." Of course, Nilsson has nothing to do with cookie blocking; rather, the entire point of that scheme is to store cookies at the proxy so that they do not have to be returned to the requested end user terminals. Stated another way, in Nilsson there is no cookie blocking function because the whole purpose of the proxy is to store the server-generated cookies. There is no function in Nilsson that selectively "block[s] transmission of cookies" (and then, conversely, allows such cookies to pass back through the proxy). In particular, an end user of the terminal 52 cannot configure the proxy 66 in any way to allow, let alone to allow some cookies to pass through while others are merely stored.

As can be seen, Nilsson simply teaches cookie storage in the proxy to obviate passing the cookie back to the requesting end user terminal, and then later re-using the cookie to obtain access to a resource on the server. This is not the subject matter of the claims here. Rather, the claims here assume that the client has obtained access to the server and that the server has issued the cookie. Unlike the cited art, the claims concern whether that cookie will be returned to the client. As noted above, no cookies are ever returned to the requesting end user terminals 52 in the Nilsson scheme. This cookie processing concept is not disclosed or suggested by any of the art of record, as none of the references even address the question of how a cookie being returned from a server to the client should be processed, let alone filtered according to user-configurable options. In particular, the cited prior art does not describe providing a technique for enabling a user to configure at the proxy server per-domain (and, optionally, per-client profile) filtering of cookies that are returned from servers. Rather, the cited prior art deals with an unrelated issue,

*viz.*, how to store and re-use a cookie so that the requesting end user terminal does not need to store it directly.

For the reasons set forth above, the combination of the cited art still fails to disclose at least the following steps of claim 1:

"receiving a set of parameters in a client message at the proxy server, wherein the set of parameters are configured by the user at the client;

storing the set of parameters at the proxy server, wherein the parameters comprise domain identifiers associated with indications of whether to block transmission of cookies associated with the domain identifiers;

extracting from the response message a domain identifier associated with the server;

retrieving the set of parameters; and

processing the cookie at the proxy server in accordance with the retrieved set of parameters and the extracted domain identifier."

As the prior art does not disclose "processing the cookie" in accordance with the "retrieved set of parameters and the extracted domain identifier." This user-configurable per-source domain "filtering" provides an enhanced privacy service that is neither disclosed nor suggested by the prior art. Thus, independent claims 1 (method), 10 (apparatus) and 19 (computer program product) describe patentable subject matter.

Dependent claims 2, 11 and 20 describe the cookie filtering steps more specifically and, in particular, the steps of blocking the cookie from transmission, caching the cookie at the proxy, and sending a modified response message to the client. This is the scenario such as described in steps 614, 618 and 620 of FIG. 6A, where the user has selected an option not to allow the cookie through the privacy service proxy server. As noted above, Nilsson has no concept of selectively blocking some cookies while allowing others to pass back through to the client. These claims are separately patentable because the cited art does not teach any filtering of cookies being returned from a server to a client, let alone the specific requirements set forth in these claims.

Dependent claims 3, 12 and 21 likewise describe the cookie filtering steps but in this case describe the operation where the cookie (of a recognized domain) is passed back to the client. This is the scenario such as described in step 614 and 616 of FIG. 6A, where the user has selected an option to allow the cookie through the privacy service, in which case the privacy

service sends the response to the client without removing or detaching the cookie from the response. These claims likewise are patentable over the cited references, which do not teach any response cookie filtering. Indeed, Nilsson teaches away from this requirement, *as cookies are retained at and by the proxy.*

Dependent claims 5, 14 and 23 are separately patentable as they describe the further step of determining if the set of parameters contains an indication that the user has enabled cookie processing by the proxy server. In one embodiment, this refers to determining whether a "source domain filter enable flag" (218) is set. The cited art does not perform cookie filtering, so this functionality is also absent from any combination of the references.

Dependent claims 6, 15 and 24 are separately patentable as they describe the further steps of managing the "multiple set of parameters." This is a client profile option. The references do not disclose or suggest cookie filtering on a per-domain basis, thus they cannot teach the further features recited in these claims.

Dependent claims 7-9, 16-18 and 25-27 are patentable for the reasons advanced with respect to their parent claims.

A Notice of Allowance is respectfully requested.

Respectfully submitted,

/David H. Judson/

By: _____

David H. Judson, Reg. No. 30,467